UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/928,290	08/10/2001	Mukesh Sharma	70236	6996

7590 09/06/2005

McGLEW AND TUTTLE, P.C.
SCARBOROUGH STATION
SCARBOROUGH, NY 10510-0827

EXAMINER	
RYMAN, DANIEL J	
ART UNIT	PAPER NUMBER
2665	

DATE MAILED: 09/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/928,290	SHARMA ET AL.	
	Examiner	Art Unit	
	Daniel J. Ryman	2665	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☒ Claim(s) *5, 15, 16, and 18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 August 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information submitted for consideration by the Office, and MPEP § 609 A(1) states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless the references have been cited by the examiner on form PTO-892, they have not been considered. Specifically, Applicant should include the references on pg. 4, lines 8-10, pg. 6, lines 12-14, and pg. 14, lines 10-12, in an IDS.

Drawings

2. The drawings are objected to because in Fig. 6, "6nnnn: should be "6" and in Fig. 2 "Luis prefers using something other than IKE (Kerberos)" should be deleted. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR

1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The abstract of the disclosure is objected to because it exceeds 150 words in length. Correction is required. See MPEP § 608.01(b).

4. The disclosure is objected to because of the following informalities: on page 16, line 18, "The" should be "the".

Appropriate correction is required.

5. Examiner requests that Applicant update the application information on page 13, lines 5-8 to reflect any changes in the status of these applications.

Claim Objections

6. Claim 5 is objected to because of the following informalities: "MN 2" should be "MN". Appropriate correction is required.

7. Claims 15, 16 and 18 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Examiner suggests changing the dependency of claim 14 from claim 10 to claim 13.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 10-12 and 14-19 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

10. A broad range or limitation together with a narrow range or limitation that falls within the broad range or limitation (in the same claim) is considered indefinite, since the resulting claim does not clearly set forth the metes and bounds of the patent protection desired. Note the explanation given by the Board of Patent Appeals and Interferences in *Ex parte Wu*, 10 USPQ2d 2031, 2033 (Bd. Pat. App. & Inter. 1989), as to where broad language is followed by "such as" and then narrow language. The Board stated that this can render a claim indefinite by raising a question or doubt as to whether the feature introduced by such language is (a) merely exemplary of the remainder of the claim, and therefore not required, or (b) a required feature of the claims. Note also, for example, the decisions of *Ex parte Steigewald*, 131 USPQ 74 (Bd. App. 1961); *Ex parte Hall*, 83 USPQ 38 (Bd. App. 1948); and *Ex parte Hasche*, 86 USPQ 481 (Bd. App. 1949). In the present instance, claim 10 recites the broad recitation "at least one ... of a connection from the MN to the SGPRS and a connection between the MN and WLAN", and the claim also recites "both of a connection from the MN to the SGPRS and a connection between the MN and WLAN" which is the narrower statement of the range/limitation. For the purposes of prior art rejections, Examiner will interpret the claim to read "at least one of a connection from the MN to the SGPRS and a connection between the MN and WLAN."

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1-12 and 14-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barnes et al. (USPN 6,711,147) in view of Yokote (PGPub 2002/0157024) in further view of Yuan (USPN 6,496,704).

13. Regarding claim 1, Barnes discloses a wireless data network process, comprising the steps of: providing a wireless local area network (WLAN) (ref. 202: mobile IP based network) with a wireless access node, an internet connection and a mobile node (MN) with a wireless transceiver (col. 6, lines 57-67); providing a GPRS support node (GSN) having a connection to the internet (Fig. 4 and col. 4, lines 29-41).

Barnes does not expressly disclose providing a serving GPRS support node with a radio network connection to a Gateway GPRS support packet gateway node (PGN) having a connection to the internet. However, Barnes does disclose providing a GPRS support node (GSN) having the functionality of a serving GPRS node and a gateway GPRS node (col. 7, lines 38-46). Barnes also discloses as prior art providing a serving GPRS support node with a radio network connection to a Gateway GPRS support packet gateway node (PGN) having a connection to the internet (Figs. 1a and 3; col. 2, lines 16-29; col. 2, lines 45-53; and col. 6, line 32-col. 7, line 13). It is implicit that by modifying only the GGSN to include the functionality of the HA/FA, rather than including the SGSN, the GGSN, and the HA/FA in a single node, legacy radio networks can be modified to support mobile IP at a minimal cost. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to provide a serving GPRS

support node with a radio network connection to a Gateway GPRS support packet gateway node (PGN) having a connection to the internet since this is the prior art structure for a radio network.

Barnes does not expressly disclose performing a key exchange between the MN and the PGN via radio waves, the GPRS support node and the connection to establish a shared secret key and to establish an IPsec Security Association (SA) between the MN and the PGN or using a security parameters index obtained from the SA for identifying the MN. However, Barnes does disclose using IPSec to ensure security (col. 4, lines 13-18) over the IP-tunnels (Fig. 4). Barnes also discloses that information is exchanged between the MN and the PGN via radio waves, the GPRS support node and the connection (Figs. 1a and 3; col. 2, lines 16-29; col. 2, lines 45-53; and col. 6, line 32-col. 7, line 13). Yokote teaches, in a wireless system that supports Mobile IP and IPsec, performing a key exchange between the home agent and the mobile node (¶¶ 11-13) to ensure secure communications over the tunnel (¶ 13). Yokote also teaches using an SPI to identify an MN (¶ 13). Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to perform a key exchange between the MN and the PGN (GSN/HA in Barnes) via radio waves, the GPRS support node and the connection to establish a shared secret key and to establish an IPsec Security Association (SA) between the MN and the PGN where an SPI is used to identify the MN in order to ensure secure communications over the tunnel.

Barnes in view of Yokote does not expressly disclose performing a hash of the key obtained at the PGN to obtain an authentication value for use in a Mobile IP protocol; performing a hash of the key obtained at the MN to obtain an authentication value for use in a Mobile IP protocol; sending a Mobile IP registration request from the MN to a Home Agent (HA) hosted in the PGN using the authentication value established; receiving the Mobile IP

registration request at the PGN and authenticating the message using the authentication value and sending a Mobile IP registration reply to the MN. Yuan teaches, in a wireless system that supports Mobile IP, that Mobile IP includes optional authentication extensions where an authentication key is exchanged between the nodes and subsequently hashed (col. 4, lines 43-63). Yuan also teaches that there is no mechanism specified in IP for the distribution of the authentication key (col. 4, lines 43-63), such that it would be obvious to use the keys provided in IPsec. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to perform a hash of the key obtained at the PGN to obtain an authentication value for use in a Mobile IP protocol; performing a hash of the key obtained at the MN to obtain an authentication value for use in a Mobile IP protocol; sending a Mobile IP registration request from the MN to a Home Agent (HA) hosted in the PGN using the authentication value established; receiving the Mobile IP registration request at the PGN and authenticating the message using the authentication value and sending a Mobile IP registration reply to the MN in order to provide authentication in Mobile IP using a key that has already been exchanged through the key distribution process of IPsec.

14. Regarding claim 2, Barnes in view of Yokote in further view of Yuan suggests that the step of performing a key exchange includes performing a key exchange with the MN requesting Encapsulated Security Protocol (ESP) for establishing the SA (Yokote: ¶ 48). Barnes in view of Yokote in further view of Yuan does not expressly disclose using the Internet Key Exchange (IKE) protocol; however, Examiner takes official notice that IKE is a well-known protocol used with IPsec. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the IKE protocol for key exchange.

15. Regarding claim 3, Barnes in view of Yokote in further view of Yuan suggests receiving the Mobile IP registration reply at the MN and if the ESP established is not active, activating the ESP at the MN (Yokote: ¶ 48); sending data packets from the MN to a target host on the internet using the ESP to the PGN with the PGN forwarding the packets to the target host (Barnes: col. 8, line 47-col. 9, line 37); replying by sending reply packets from the target host to the PGN with the PGN forwarding the reply packets using the ESP to the MN (Barnes: col. 8, line 47-col. 9, line 37).

16. Regarding claim 4, Barnes in view of Yokote in further view of Yuan suggests establishing a connection of the MN on the Wireless LAN (Barnes: col. 6, line 32-col. 7, line 13 and col. 8, line 47-col. 9, line 37); requesting a Mobile IP Care-Of-Address (COA) from Dynamic Host Configuration Protocol (DHCP) server on the Internet (Barnes: col. 3, lines 45-50) where it is well known to obtain an IP address from a DHCP server; receiving the COA at the MN from across the Wireless LAN, wherein said step of sending data packets from the MN to a target host is via the wireless LAN connection to the internet and said step of replying by sending reply packets from the target host to the PGN is via the internet to the wireless LAN (Barnes: col. 6, line 32-col. 7, line 13 and col. 8, line 47-col. 9, line 37).

17. Regarding claim 5, Barnes in view of Yokote in further view of Yuan suggests terminating the connection with the PGN and detatching from the WLAN after the conclusion of the data session to the MN (Barnes: col. 6, line 32-col. 7, line 13 and col. 8, lines 47-col. 9, line 37) where it is implicit that the MN will eventually terminate the session.

18. Regarding claim 6, Barnes in view of Yokote in further view of Yuan suggests roaming with the MN into a region of the radio network and sending a message from the MN a Mobile IP

registration request to the Home Agent hosted in the PGN indicating that the MN is on the home network (Barnes: col. 6, line 32-col. 7, line 13 and col. 8, lines 47-col. 9, line 37) and using the authentication value obtained within the message (Yuan: col. 4, lines 43-63); sending a Mobile IP registration reply from the PGN to the MN using the authentication value obtained (Barnes: col. 6, line 32-col. 7, line 13 and col. 8, lines 47-col. 9, line 37 and Yuan: col. 4, lines 43-63).

19. Regarding claim 7, Barnes in view of Yokote in further view of Yuan discloses that the authentication value is a 128 bit authentication value (Yuan: col. 4, lines 55-57).

20. Regarding claim 8, Barnes in view of Yokote in further view of Yuan suggests that the Mobile IP registration request can be sent via the established ESP (Yokote: ¶ 48) where this results in a secure registration request.

21. Regarding claim 9, Barnes in view of Yokote in further view of Yuan suggests that the Mobile IP registration request is sent without the established ESP (Yokote: ¶ 48) where this results in an unsecured registration request.

22. Regarding claims 10 and 18, Barnes discloses a wireless network system, comprising: a mobile node with a wireless transceiver (col. 6, lines 57-67); a radio access network (Fig. 4; col. 4, lines 29-41; and col. 7, lines 38-46); a GPRS support node (GSN) including a packet gateway node (PGN) with an internet connection, the PGN being capable of acting as a mobile IP home agent (HA) (Fig. 4; col. 4, lines 29-41; and col. 7, lines 38-46); a wireless local area network (WLAN) (ref. 202: mobile IP based network) with a wireless access node and an internet connection (col. 6, lines 57-67); at least one of a connection from the MN to the SGPRS and a connection between the MN and the WLAN (Fig. 4; col. 4, lines 29-41; and col. 7, lines 38-46).

Barnes does not expressly disclose providing a serving GPRS support node with a radio network connection to a Gateway GPRS support packet gateway node, which is capable of acting as a HA. However, Barnes does disclose providing a GPRS support node (GSN) having the functionality of a serving GPRS node, a gateway GPRS node, and a HA (col. 7, lines 38-46). Barnes also discloses as prior art providing a serving GPRS support node with a radio network connection to a Gateway GPRS support packet gateway node (PGN) having a connection to the internet (Figs. 1a and 3; col. 2, lines 16-29; col. 2, lines 45-53; and col. 6, line 32-col. 7, line 13). It is implicit that by modifying only the GGSN to include the functionality of the HA/FA, rather than including the SGSN, the GGSN, and the HA/FA in a single node, legacy radio networks can be modified to support mobile IP at a minimal cost. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to provide a serving GPRS support node with a radio network connection to a Gateway GPRS support packet gateway node (PGN) having a connection to the internet since this is the prior art structure for a radio network.

Barnes also does not expressly disclose a Mobile IP care-of-address obtained from a DHCP server through the connection between the MN and the WLAN. However, Barnes does disclose that the Mobile IP care-of-address can be obtained by the MN (col. 3, lines 45-50). Examiner takes official notice that it is well known to obtain an IP address from a DHCP server. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to obtain an IP address from a DHCP server.

Barnes does not expressly disclose performing a key exchange between the MN and the PGN using the MN to the SGPRS connection to form an IPsec Security Association (SA) between the MN and the PGN using a security parameters index obtained from the SA for

identifying the MN. However, Barnes does disclose using IPSec to ensure security (col. 4, lines 13-18) over the IP-tunnels (Fig. 4). Barnes also discloses that information is exchanged between the MN and the PGN via radio waves, the GPRS support node and the connection (Figs. 1a and 3; col. 2, lines 16-29; col. 2, lines 45-53; and col. 6, line 32-col. 7, line 13). Yokote teaches, in a wireless system that supports Mobile IP and IPsec, performing a key exchange between the home agent and the mobile node (¶¶ 11-13) to ensure secure communications over the tunnel (¶ 13). Yokote also teaches using an SPI to identify an MN (¶ 13). Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to perform a key exchange between the MN and the PGN (GSN/HA in Barnes) via radio waves, the GPRS support node and the connection to establish a shared secret key and to establish an IPsec Security Association (SA) between the MN and the PGN where an SPI is used to identify the MN in order to ensure secure communications over the tunnel.

Barnes in view of Yokote does not expressly disclose performing a MD-5 hash of the key obtained at the PGN to obtain an authentication value for use in a Mobile IP protocol; performing a MD-5 hash of the key obtained at the MN to obtain an authentication value for use in a Mobile IP protocol; sending a Mobile IP registration request from the MN to a Home Agent (HA) hosted in the PGN using the authentication value established; receiving the Mobile IP registration request at the PGN and authenticating the message using the authentication value and sending a Mobile IP registration reply to the MN. Yuan teaches, in a wireless system that supports Mobile IP, that Mobile IP includes optional authentication extensions where an authentication key is exchanged between the nodes and subsequently MD-5 hashed (col. 4, lines 43-63). Yuan also teaches that there is no mechanism specified in IP for the distribution of the

authentication key (col. 4, lines 43-63), such that it would be obvious to use the keys provided in IPsec. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to perform a MD-5 hash of the key obtained at the PGN to obtain an authentication value for use in a Mobile IP protocol; performing a MD-5 hash of the key obtained at the MN to obtain an authentication value for use in a Mobile IP protocol; sending a Mobile IP registration request from the MN to a Home Agent (HA) hosted in the PGN using the authentication value established; receiving the Mobile IP registration request at the PGN and authenticating the message using the authentication value and sending a Mobile IP registration reply to the MN in order to provide authentication in Mobile IP using a key that has already been exchanged through the key distribution process of IPsec.

23. Regarding claim 11, Barnes in view of Yokote in further view of Yuan discloses that the authentication value is a 128 bit authentication value (Yuan: col. 4, lines 55-57).

24. Regarding claim 12, Barnes in view of Yokote in further view of Yuan discloses that the request message is sent from the MN to the PGN via the WLAN and a connection from the WLAN to the PGN over the internet (Barnes: col. 6, line 32-col. 7, line 13 and col. 8, lines 47-col. 9, line 37).

25. Regarding claim 14, Barnes in view of Yokote in further view of Yuan suggests that the initial key forms the basis for subsequent key exchanges using a standard's based protocol (Yokote: ¶ 49) where the keys used with a SA expire with the SA (discrete lifetime) such that the subsequent key exchange will occur using the encrypted channel established using the initial key (basis for subsequent key exchanges).

26. Regarding claim 15, Barnes in view of Yokote in further view of Yuan discloses that the standard's based protocol is IPsec (Barnes: col. 4, lines 13-18 and Yokote: ¶¶ 11-13).

27. Regarding claim 16, Barnes in view of Yokote in further view of Yuan suggests that with a shared key in place, the Mobile IP authentication key is derived by performing an MD-5 hash of the shared key (Yuan: col. 4, lines 43-63) whereby preprogramming of the authentication key is not needed and the authentication key need not remain static (Yuan: col. 4, lines 43-63).

28. Regarding claim 17, Barnes in view of Yokote in further view of Yuan does not expressly disclose that subsequent traffic between the MN and the PGN is encrypted using an authenticated key exchange with the IKE aggressive mode key exchange (very fast) using the shared key to establish a large encryption key and an SA. However, Examiner takes official notice that IKE is well known. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have encrypt subsequent traffic between the MN and the PGN using an authenticated key exchange with the IKE aggressive mode key exchange (very fast) using the shared key to establish a large encryption key and an SA since this is well known in the art.

29. Regarding claim 19, Barnes in view of Yokote in further view of Yuan discloses that the authentication value is a 128 bit authentication value (Yuan: col. 4, lines 55-57).

30. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Barnes et al. (USPN 6,711,147) in view of Yuan (USPN 6,496,704) in further view of Yokote (PGPub 2002/0157024).

31. Regarding claim 13, Barnes discloses a wireless network system, comprising: a mobile node with a wireless transceiver (col. 6, lines 57-67); a radio access network (Fig. 4; col. 4, lines 29-41; and col. 7, lines 38-46); a GPRS support node (GSN) including a packet gateway node

(PGN) with an internet connection, the PGN being capable of acting as a mobile IP home agent (HA) (Fig. 4; col. 4, lines 29-41; and col. 7, lines 38-46).

Barnes does not expressly disclose providing a serving GPRS support node with a radio network connection to a Gateway GPRS support packet gateway node which is capable of acting as a HA. However, Barnes does disclose providing a GPRS support node (GSN) having the functionality of a serving GPRS node, a gateway GPRS node, and a HA (col. 7, lines 38-46). Barnes also discloses as prior art providing a serving GPRS support node with a radio network connection to a Gateway GPRS support packet gateway node (PGN) having a connection to the internet (Figs. 1a and 3; col. 2, lines 16-29; col. 2, lines 45-53; and col. 6, line 32-col. 7, line 13). It is implicit that by modifying only the GGSN to include the functionality of the HA/FA, rather than including the SGSN, the GGSN, and the HA/FA in a single node, legacy radio networks can be modified to support mobile IP at a minimal cost. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to provide a serving GPRS support node with a radio network connection to a Gateway GPRS support packet gateway node (PGN) having a connection to the internet since this is the prior art structure for a radio network.

Barnes does not expressly disclose performing authentication of a MN handled by the GPRS/UMTS network before the PGN ever sees data traffic to establish a Mobile IP authentication key, wherein an unauthenticated key exchange method such as Diffie-Hellman can be used to establish the shared key. Yuan teaches, in a wireless system that supports Mobile IP, that Mobile IP includes optional authentication extensions where an authentication key is exchanged between the nodes (col. 4, lines 43-63). Yuan also teaches that there is no mechanism specified in IP for the distribution of the authentication key (col. 4, lines 43-63). Yokote teaches,

in a wireless system that supports Mobile IP and IPsec, generating a key using Diffie-Hellman (¶ 12) to ensure secure communications over the tunnel (¶ 13). Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to perform authentication of a MN handled by the GPRS/UMTS network before the PGN ever sees data traffic to establish a Mobile IP authentication key, wherein an unauthenticated key exchange method such as Diffie-Hellman can be used to establish the shared key in order to provide authentication using a key that is provided by IPsec.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel J. Ryman whose telephone number is (571)272-3152. The examiner can normally be reached on Mon.-Fri. 7:00-4:30 with every other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on (571)272-3155. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HUY D. VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600

DJR

Daniel J. Ryman
Examiner
Art Unit 2665